

**AFFIDAVIT**

I, Carlos Suarez, (hereinafter “Your Affiant”), being duly sworn, state the following is true and correct to the best of my knowledge and belief:

1. Your Affiant is a Special Agent (SA) with the United States Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), currently assigned to the Kansas City, Missouri office since August 15, 2010. Prior to my employment with HSI, I worked for approximately three years as a Border Patrol Agent with Customs and Border Protection (CBP). During this time, your Affiant has investigated various “white collar” crimes, including but not limited to, wire fraud, mail fraud, bank fraud, money laundering and visa fraud. Your Affiant is a graduate of the Federal Law Enforcement Training Center’s Basic Border Patrol Agent Training Program, the Criminal Investigator Training Program and the Immigration and Customs Enforcement Special Agent Training Program.

2. This affidavit is made in support of an application for six (6) warrants authorizing the electronic searches of the following TARGET ITEMS in LIU’s possession as he made entry into the United States and was subsequently arrested on an arrest warrant issued in the Western District of Missouri.<sup>1</sup>:

- a. An Apple MacBook Air (Serial Number C02NCBK0G083), identified as TARGET ITEM 1 (Search Warrant No. 16-SW-00175-JTM);
- b. A Huawei cellphone (Model No. NXT-AL10), identified as TARGET ITEM 2 (Search Warrant No. 16-SW-00176-JTM);

---

<sup>1</sup>Many of the facts detailed in this affidavit are also contained in the affidavit supporting the criminal complaint filed against Wen Tao Liu on June 13, 2016. *See United States of America v. Wen Tao Liu, a/k/a Orland Liu, d/b/a Haitu International Group Co. Limited*, Case No. 16-MJ-00115-JTM. (Doc. No. 1).

- c. A China Merchants Bank Thumb Drive, with identifying number 2332193649, identified as TARGET ITEM 3 (Search Warrant No. 16-SW-00177-JTM);
- d. A ScanDisk Cruzer Blade Thumb Drive, with identifying number BM160225243B, identified as TARGET ITEM 4 (Search Warrant No. 16-SW-00178-JTM);
- e. A Kingston DTSE9 Thumb Drive, with identifying number 7158942, identified as TARGET ITEM 5 (Search Warrant No. 16-SW-00179-JTM);
- f. A Kingston DataTraveler Locker+ G2 Thumb Drive, identified as TARGET ITEM 6 (Search Warrant No. 16-SW-00180-JTM);

3. Based upon your Affiant's review of the evidence to date, and as set forth below, your Affiant believes the aforementioned TARGET ITEMS, contain items which constitute evidence, fruits, and instrumentalities of violations of federal law, namely, unauthorized solicitation of access devices in violation of 18 U.S.C. § 1029(a)(6); trafficking in counterfeit goods in violation of 18 U.S.C. § 2320; and smuggling goods into the United States in violation of 18 U.S.C. § 545.

4. I am familiar with the information contained in this affidavit based upon the investigation I have conducted, along with my conversations with law enforcement officers and others and review of reports and database records.

5. This affidavit is submitted for the limited purpose of securing a search and seizure warrant. It does not include each and every fact known to me or the Government about the investigation. I have set forth only those facts that I believe are necessary to establish probable cause.

#### **Summary of the Investigation**

6. Based on the evidence gathered in the course of this investigation, your affiant has probable cause to believe that, from at least 2010 to the present, LIU has fraudulently obtained and sold counterfeit, illicit, and/or unauthorized Microsoft software, software products, and related components, including unauthorized product key codes and counterfeit product key cards,

causing the Microsoft Corporation millions of dollars in losses. In the course of this conspiracy, LIU has been identified as a primary source of supply and believed to be a “harvester” of illicit and unauthorized product key codes operating in the People’s Republic of China (PRC). These harvesters collect product key codes which are sold over and over, to resellers in the United States and other countries, which negatively affect the end-user or consumer by ultimately receiving illicit or unauthorized product key codes or codes that will have been blocked by the time an end-user attempts to activate them. Harvesters are believed to obtain these products by illicit means, in the execution of various schemes designed to defraud the Microsoft Corporation and the various programs it operates (such as abuses of the educational system codes or those sold with operating systems). After acquiring the unauthorized product key codes, LIU would then send these codes via digital transmission, including e-mail, and/or would facilitate the transfer of these codes onto counterfeit products for sale to various resellers in the United States, including those within the Western District of Missouri.

7. In the course of this investigation, HSI special agents based in Kansas City, Missouri, learned in mid-2013 that CASEY LEE ROSS, of Kansas City, Missouri, which is within the Western District of Missouri, had purchased (and redistributed) tens of thousands of unauthorized Microsoft product key codes and counterfeit product key cards from suspect sources in the People’s Republic of China. These product key codes were purchased from suspect sources at prices well below that of the Estimated Retail Price (“ERP”), had to be continually checked by ROSS and others to verify that the limited number of activations had not been used or that they had not been blocked by Microsoft, and, in many cases, were distributed on counterfeit card stock intended to make it appear as if they were genuine Microsoft products. ROSS then distributed large quantities of these product key codes and counterfeit Microsoft

product key cards to various co-conspirators within the United States, who in turn sold the product key codes and counterfeit product key cards through their respective websites as well as on e-commerce sites such as eBay or Amazon.com.

8. HSI agents learned that ROSS was principally supplying numerous individuals who, in turn, were all engaged in the business of selling these unauthorized product key codes and counterfeit product key cards for Microsoft software products to unsuspecting customers. HSI investigators learned that ROSS was conspiring with numerous co-conspirators, including INDIVIDUAL H in the United States, as well as others, to execute this scheme.

9. Your Affiant determined, based on a review of email communications as well as financial documentation, that LIU and his company, HAITU INTERNATIONAL GROUP CO. LIMITED (“HIG”) were one of ROSS’s principal suppliers of these unauthorized product key codes and counterfeit product key cards.

10. Your Affiant further states that numerous individuals that have obtained these unauthorized product key codes and counterfeit product key cards from LIU and HIG, or have engaged in numerous communications with LIU and HIG, have pled guilty before Chief United States Judge Gregory Kays relating to their role in this expansive software piracy investigation. *See United States v. Casey Lee Ross*, No. 15-00196-01-CR-W-DGK, *United States v. Matthew Lockwood*, Case No. 15-00197-CR-W-DGK, *United States v. Arunachalam Annamalai*, Case No. 15-00242-CR-W-DGK, *United States v. Reza Davachi*, Case No. 15-00346-01-CR-W-DGK, *United States v. Jake Schwartz*, Case No. 15-00347-01-CR-W-DGK, and *United States v. Rex Yang*, No. 15-00392-01-CR-W-DGK.

**LIU and HAITU INTERNATIONAL GROUP CO. LIMITED**

11. Your Affiant is aware Wen Tao LIU is a citizen and national of the People Republic of China (PRC). LIU also has a United States non-immigrant visa issued on January 14, 2015, category B1/B2 (Visitor). Department of Homeland Security (DHS) databases reveal LIU presented a PRC Passport, number E19956782, a PRC National ID of 430524198005053254, when applying for his visa, and claimed a date of birth of May 5, 1980, born in Shaoyang, PRC. LIU also claimed an employer of Shenzhen Yisimeng Jewelry Co. Limited, and an email address of luu245@126.com.

12. Your Affiant has also received information from Special Agents (SAs) with the Federal Bureau of Investigation (FBI), obtained through the Mutual Legal Assistance Treaty (MLAT) process concerning a bank account opened by LIU at a HSBC Bank local in Shenzhen, Guangdong, PRC. The document, described as a Business Integrated Account Opening Form, relating to account number 509-791869-838, contains information provided by LIU when opening a business account for his company, Haitu International Group Co. Limited (“HIG”). In the document, dated March 26, 2010, LIU lists a Certificate of Incorporation number as 1428423, registered on March 10, 2010, in Hong Kong. In a field on the form requesting the Country of Source of Funds, LIU listed “USA, Dubai [and] Australia.” Additionally, in the company and account information section, LIU’s job title is listed as Director, with office phone number of 755-29194170 and an email address of luu245@gmail.com. The document was accompanied by the copies of LIU’s identification listing a PRC National ID of 430524198005053254, witnessed and signed by officers of the bank.

13. Your Affiant is aware Haitu International Group Co. Limited (“HIG”) is a Hong Kong company which operates and maintains the website [www.haitugroup.com](http://www.haitugroup.com). Your Affiant’s review of the website revealed tabs at the top of the page, one of which is called “Contact Us.”

This tab resolves to a web page which notes two offices associated with HIG, one located in Shenzhen, PRC, and the other in Hong Kong. The webpage lists “Orland Liu” as the contact person, with an email of sales@haitugroup.com, and a Microsoft Network (MSN) email address of luu245@hotmail.com.

**Information Provided by Affected Software Developers Regarding LIU and HIG**

14. Throughout the investigation, your Affiant has received information from Microsoft and Adobe concerning the product key codes associated with the resellers, analysis on the counterfeit product and previous encounters with the targets of the investigation. Your Affiant is aware Microsoft and Adobe maintain databases with the information of individuals whom they suspect of selling and distributing counterfeit and infringing products, both in the United States and in countries abroad, primarily for evidentiary support in civil proceedings against these individuals. The following is information maintained Microsoft and Adobe concerning HIG and shared with your Affiant.

15. Your Affiant received information from Microsoft fraud representative concerning HIG, specifically associated with a shipment of products intercepted by Australian customs officials, originating with HIG. The shipment, intended for Ibrahim SHAMAS, 40 Greenshank Road, in Harrisdale, Australia, was accompanied by a commercial invoice describing the goods as 50 pieces of “Technical Material” worth \$200.00. In a Deed of Undertaking, completed and signed by SHAMAS, he claims to have purchased 50 DVD Learning Tutorials on how to use the software program known as Microsoft Windows 7. All of the items within the shipment were deemed to be counterfeit by Microsoft fraud representatives. An example of one of the counterfeit discs in this shipment is shown below:



16. Your Affiant also received information concerning HIG from fraud representatives with Adobe. In a sworn declaration filed with the Adobe litigation filed in United States District Court for the Northern District of California, Case No. 5:14-CV-02147-LHK (*Adobe Systems Incorporated v. Softwaremedia.com, Inc., et al.*), Shijun XIAO made numerous declarations relating to the origination of his infringing and illicit software. In his declaration, which was executed on November 18, 2015, in Brooklyn, New York, XIAO stated he was the president of United Prospect, Inc. (“UP”), and was in the business of buying and selling computer software. XIAO stated he purchased, and subsequently sold and distributed approximately 270 units of Adobe-branded software. XIAO further stated that he purchased this Adobe-branded software exclusively from Haitu International Co. Ltd. XIAO stated the company used the email sales1@haitugroup.com, a business website of www.computer-system-software.com, and he received purchase orders which contained the name “Sunshine.”

17. Adobe representatives confirmed to your Affiant that the Adobe software serial keys referenced in the XIAO declaration were stolen, and were part of a larger volume of

products that were stolen from their distribution channel, and were never ultimately sold to the public.

**Relevant Email Communications Involving LIU and HIG**

18. Your Affiant has reviewed numerous email accounts through the execution of search warrants issued in the Western District of Missouri, in furtherance of this investigation. LIU, and his company HIG, have been identified on numerous occasions as the source of counterfeit and illicit products resold in the United States. Your Affiant has identified at least 4,659 individual product activation key codes distributed by LIU to various resellers in the United States. Those 4,659 codes were analyzed by Microsoft fraud representatives at your Affiant's request. Microsoft representatives confirmed the codes activation history exhibited signs of abuse, as the codes were collectively activated over 36,000 times. Additionally, Microsoft found they had already blocked 1,111 of those keys due to suspicions of piracy and 2,267 of the keys were already identified in the course of other Microsoft fraud investigations. The activation of the 4,659 product keys represents a baseline loss to the Microsoft Corporation of approximately \$1,157,250. Based on the number of unauthorized activations, the total loss, to date, could total approximately \$9 million from this universe of unauthorized product key codes.

19. In the course of this investigation, your Affiant observed numerous email communications between LIU/HIG and other individuals involved in this software piracy conspiracy, including ROSS (at all times based in the Western District of Missouri) and others. The following is a sample of the email communications between LIU/HIG and the resellers identified throughout this investigation:

20. In an email reply dated May 22, 2013, from "Sunshine" (sales1@haitugroup.com) and "softwareslasher" (ROSS), the body of the email states "Hello Casey, Please see the



attachment of Office 2010 pro Lenovo card invoice.” The body of the email also contained a signature block with the name “Sunshine,” the company name Haitu International Group Co., Ltd, and the product website [www.computer-system-software.com](http://www.computer-system-software.com). The attachment is a Performa invoice, for one-hundred (100) Office 2010 Professional Lenovo Cards, sold at \$85 each. The invoice also describes the bank information for payment as the Hong Kong and Shanghai Banking Corporation (HSBC) Limited, the beneficiaries name as Haitu International Group Co. Limited, and the account number as 509-791869-838.

21. The aforementioned attached invoice lists the seller as “Sunshine Liu” with “Haitu International Group Co. Ltd.” and, elsewhere in the invoice, lists the responsible signing individual as “Orland Liu.” Your Affiant attests that LIU has interchangeably used the nicknames “Sunshine” and “Orland” in the observed communications in the course of this investigation. Further, the bank account provided in this invoice which lists both “Sunshine” and “Orland” was created by “Wen Tao Liu” on behalf of HIG in March of 2010.

22. Your Affiant has recovered numerous counterfeit “Lenovo” product key cards in the course of this investigation. Your Affiant is further aware that counterfeiters such as LIU have used both Microsoft and Lenovo trademarks and images on these manufactured cards to add a patina of legitimacy to these counterfeit creations. Your Affiant and others with Homeland Security Investigations have conferred with fraud representatives for Microsoft Corporation and Lenovo, and have confirmed that these “Lenovo” Microsoft product key cards are not created or authorized by either company and are counterfeit.

23. In an email reply dated May 28, 2013, from “Sunshine” ([sales1@haitugroup.com](mailto:sales1@haitugroup.com)) to “softwareslasher” (ROSS) the body of the email states “Hi Casey, For the Lenovo card: the tracking number is DHL#: 7262098701 (now already arrived USA, will arrive your address

soon.) For the PKC: now it will via HK EMS, because the DHL now is more and more strict with the custom, today the PKC parcel was returned by the DHL, so we have to change it via the HK EMS. Hope you kindly understand us. And we guarantee HK EMS is safe, can smooth pass the custom, also the delivery time is most fast than ordinary EMS, so it also fast. When we ship well the PKC and get the tracking number, I'll send it to you at once. Much thanks for you so kindly waiting. Best regards, Sunshine.”

24. Your Affiant is believes that the above communication between ROSS and LIU is an acknowledgment of their past experiences with customs seizing counterfeit and infringing shipments, and goes to their efforts to smuggle and import goods into the United States in violation of 18 U.S.C. § 545.

25. In an email reply dated January 6, 2014, from INDIVIDUAL H to “Orland Liu,” the body of the email states “Orland, The list of Office 2010 HB you sent me has 2 problems! The keys are duplicated twice in [this] list (ten (10) product activation key codes listed). The keys below you have already sent me before (seven (7) product activation key codes listed)! Please send 20 replacements ASAP!” In reply, “Orland” (orland@haitugroup.com) to INDIVIDUAL H, writes “Hi...Yes they are duplicate keys, but these 10pcs keys are brand new key. For the 50 pcs I sent, each key can be activated for 1 PC online, so no problem. Important, the 2010 HB FPP key is difficult to obtain, not like other product, when you need 30 pcs, then we send 30 pcs. We'd better stock some of them, for example, we take 500 or 1000 pcs in on time, and we can sell them for 2-3 months. It will be better for all of us. Best regards. Orland.”

26. Your Affiant believes the above-referenced email communications between INDIVIDUAL H and LIU goes to their knowledge as to the duplicative sales and unauthorized solicitation of these product key codes, in violation of 18 U.S.C. § 1029(a)(6).

27. Your Affiant's review of INDIVIDUAL H's various email accounts, retrieved from search warrants issued in the Western District of Missouri, resulted in the identification of the Internet Protocol (IP) information associated with the sender. One particular email contained the dynamic IP address of 73.46.161.227 on numerous days, including October 23, 2014. HSI Kansas City Special Agents provided a Customs Summons to the Comcast Legal Response Center, the entity who deals with all legal inquiries for the internet service provider (ISP), requesting subscriber information associated with the aforementioned IP address, on the date of October 23, 2014. In their reply, received March 10, 2015, the IP address resolved to an active account owned by INDIVIDUAL H, with a physical address in Fort Lauderdale, Florida.

28. On April 15, 2015, HSI Special Agents went to INDIVIDUAL H's address to execute a search warrant issued out of the United States District Court for the Southern District of Florida. At that point in the investigation, your Affiant was aware that INDIVIDUAL H had received numerous incoming packages in the short time he had lived at that address, and that INDIVIDUAL H had received approximately seven international shipments of suspected counterfeit software.

29. After the search warrant was executed at INDIVIDUAL H's residence, at approximately 1100 HRS, your Affiant and another Special Agent with Homeland Security Investigations sat down with INDIVIDUAL H and asked him if he would be willing to answer some questions. INDIVIDUAL H agreed, waiving his right to an attorney. During the interview, INDIVIDUAL H confirmed receipt of the counterfeit Lenovo cards and unauthorized product activation key codes from a distributor in Hong Kong, known to him as Orland LIU, operating a company known to him as Haitu International Group.

#### **UNDERCOVER COMMUNICATIONS AND PURCHASE**

30. On July 13, 2015, your Affiant, acting in an undercover capacity, sent an email to orland@haitugroup.com, inquiring about the production and purchase of Microsoft branded product key cards. Specifically, this order entailed LIU's creation and manufacture of counterfeit product key cards which are not produced by the Microsoft Corporation, any of its subsidiaries, contractors or affiliates. In essence, the product key card would be a counterfeit production of a product that is not sold in this manner by the Microsoft Corporation, using known trademarks of Microsoft Corporation and Lenovo. In an email response by "Orland" on July 15, 2015, he claims the Minimum Order Quantity (MOQ) for customization is 2000pcs at \$105 per card.

31. On September 16, 2015, your Affiant sent another email to "Orland" cancelling the original order, and instead requesting 500pcs of Microsoft 2010 Office Professional Lenovo product key cards, with an associated cost of \$70 per card. Due to extensive communications with fraud investigators with Microsoft Corporation, your Affiant was aware all "Lenovo" branded Microsoft 2010 Office Professional cards are counterfeit. In an email reply, Orland stated he could fill the order and relayed his bank information as follows:

Haitu T/T Bank Information

Bank Name: The Hong Kong and Shanghai Banking Corporation Limited

Bank Address: No. 1 Queen's Road Central, Central Hong Kong

Beneficiary Name: Haitu International Group Co., Limited.

Beneficiary Account No.: 509-791869-[REDACTED]

Swift Code: HSBCHKHCHKH

Bank Code: 004

32. On October 1, 2015, a wire transfer was sent to the information listed above, in the amount of \$35,000. On October 5, 2015, "Orland" confirmed, via an email to your Affiant, receipt of the wire transfer, and asked for an address where the items could be shipped. On October 7, 2015, in an email communication, "Orland" listed DHL tracking number

8313746044, as the tracking number for “500pcs cards.” The package was received by agents with HSI Kansas City on October 13, 2015. Your Affiant, observing the exterior of the package, found a commercial invoice which described the goods as “gift cards,” with a total value of \$50. Your Affiant, after taking pictures of the package, opened the box to find five-hundred (500) Lenovo branded 2010 Microsoft Office Professional product key cards wrapped in plastic. SA Suarez took pictures of the cards and packaging and sent them to Microsoft representatives for evaluation. Additionally, the contents of the package are recorded on CBP Form 6051S – #2780552.

33. On October 14, 2015, in an email response from Cindy Yard, a Microsoft Product Identification Specialist, it was confirmed the cards are in fact counterfeit. Your Affiant further states that these Lenovo cards appear very similar to other known counterfeit “Lenovo” product key cards obtained from other defendants in the course of this investigation.



### **Statutory Violations**

34. Your Affiant asserts that there is probable cause to believe that LIU, doing business as HIG, has conspired with ROSS, LOCKWOOD, ANNAMALAI, YANG, SCHWARTZ, DAVACHI, and INDIVIDUAL H to commit various offenses against the United States involving this software piracy conspiracy. Specifically, the act of creating the aforementioned counterfeit product key cards implicates violations of Title 18, including Section 1343 (wire fraud, in causing the transmissions to facilitate this fraudulent scheme and containing these unauthorized product key codes), Section 2318 (trafficking in counterfeit labels, documentation, and packaging, vis-à-vis the manufacturing of the counterfeit “Lenovo” cards), Section 2320 (trafficking in counterfeit goods, with the trafficking of said “Lenovo” cards), and Section 545 (smuggling goods into the United States, in intentionally mislabeling these international shipments to evade detection). Moreover, the ongoing trafficking in these illicit and unauthorized product key codes implicates 18 U.S.C. §§ 1343 and 1029(a)(6) (unauthorized solicitation of access devices, in the selling of these unauthorized product key codes).

**LIU’s ARREST AND SEARCH INCIDENT TO ARREST**

35. On June 14, 2016, at approximately 0500 HRS, LIU was encountered by U.S. Customs and Border Protection Officers (CBPOs) at the Dallas-Ft. Worth (DFW) International Airport, as he entered the terminal. LIU was informed there was a warrant for his arrest, issued in the Western District of Missouri, and was taken into custody. During the search incident to LIU’s arrest, your Affiant found one (1) laptop, one (1) cellphone and four (4) thumb drives among LIU’s carry-on backpack. Your Affiant recorded these items on the appropriate evidence form and informed LIU of the seizure. Your Affiant contacted a Chinese Mandarin interpreter Sky Yeung, who communicated all of the previous information, in case there was any confusion

due to a language barrier. LIU was held at the Euless City Jail pending his first appearance, scheduled for the following day.

36. Upon arrest, LIU denied any knowledge as to the passwords for the aforementioned TARGET ITEMS that were seized from him.

37. Your Affiant further states that in the course of this investigation, it appears that the identified coconspirators communicated with LIU almost exclusively via digital transmissions, using such means as email or Internet-based chat communications. Further, these Internet-based communications are the principal means by which your Affiant communicated with LIU. Your Affiant believes that these TARGET ITEMS would contain evidence which would include LIU's communications with other known and unknown coconspirators, as well as LIU's sources of the illicit and illegal software contraband.

38. On June 15, 2016, at approximately 1440 HRS, LIU was presented before U.S. Magistrate Judge Jeffrey L. Cureton, in the United States District Court for the North District Court of Texas, Fort Worth Division. LIU waived his identity hearing and signed a 5(c) Rule waiver, requesting a detention hearing in the Western District of Missouri.

39. Your Affiant reviewed the bank account information that was used to create LIU's HIG bank account with the Hongkong and Shanghai Banking Corporation Limited (HSBC). LIU created this bank account in March of 2010. In the contact information provided, LIU lists himself as the sole director and point of contact for this entity. Despite numerous opportunities to designate others as having access to this account, LIU opted not to. LIU lists no other directors or owners of this entity. In fact, on two occasions within these opening documents LIU states he has a "100%" ownership of HIG.

40. Due to the fact that LIU appears to be the sole owner and employee of HIG, and has communicated exclusively with your Affiant and other coconspirators over the Internet and via email and chat communications, your Affiant believes that there is probable cause to believe that the TARGET ITEMS he had in possession at the time of his arrest would have been used in the commission of these offenses. The nature of his business and apparent status as a sole proprietor makes any distinction between what would conventionally be considered a “business” or company-issued device or a personal one inconsequential, as any device LIU possessed would also be presumably used to engage in his ongoing illicit and illegal trade. It is reasonable to assume that LIU used the aforementioned TARGET ITEMS to conduct his business – which would include accessing these email clients and internet chat programs – and that these devices would contain evidence of said communications. Moreover, given the long length of LIU’s travel – from May 21 through June 15, 2016 – it is reasonable to assume that, at times, LIU would have used these devices to conduct business or respond to inquiries over this time. Your Affiant states that LIU has been immediately responsive to previous communications in the course of this investigation.

#### **Overview of Software Piracy Violations**

41. Your Affiant is aware that Microsoft Corporation (“Microsoft”) is a Washington corporation with its principal place of business located at One Microsoft Way, Redmond, Washington. Microsoft develops, markets, distributes, and licenses computer software programs. These software programs have included, but are not limited to the following, many of which are or have been licensed as home, professional or student/academic versions: Windows 8.1, Windows 8, Windows 7, Windows Vista, Microsoft Office, Microsoft Office Home and Business, Microsoft Office Professional, Microsoft Office for Mac, Microsoft Office for Mac



Home and Business, Microsoft Office for Mac Home and Student, Microsoft Visio, Microsoft Access, Microsoft Excel, and Microsoft Word, among others.

42. Your Affiant is further aware that Adobe Systems Incorporated (“Adobe”) is a California corporation with its principal place of business located at 345 Park Avenue, San Jose, California. Like Microsoft, Adobe also develops, markets, distributes, and licenses computer software programs. These software programs have included, but are not limited to, the following, many of which are or have been licensed as retail, professional or student/academic versions: Adobe Acrobat, Adobe After Effects, Adobe Director, Adobe Dreamweaver, Adobe Fireworks, Adobe Flash, Adobe Illustrator, Adobe InDesign, Adobe Photoshop, and Adobe Premiere, among others.

43. Your Affiant is further aware that software that is distributed by Microsoft and Adobe on physical media to its intended customers or authorized distributors (whether it is boxed for retail or accompanies a computer or computer hardware) will be distributed with a label, documentation, or packaging designed to be affixed to, enclosing, or accompanying the physical media, or to a computer or computer hardware that contains the copy of the copyrighted computer program. These labels, documentation, and packaging are distributed along with copies of the copyrighted computer programs to demonstrate that the copy of the computer program is genuine, and to signal the authorized transfer of a license to the intended end user that its use is non-infringing.

44. Your Affiant is further aware that Microsoft and Adobe also distribute their software products using a variety of distribution channels. One method of distribution employed by Microsoft is via digital download. There are a limited number of sites where customers can legally purchase digital downloads of Microsoft or Adobe software. Customers may purchase

digital downloads of Microsoft or Adobe software directly from these companies, or only through authorized retailers, or its authorized retail partners provide an Internet link that allows the customer to download a copy of the software, which is then unlocked through the entry of a product key code or serial number, as described below.

45. Your Affiant is further aware that software developers such as Microsoft and Adobe license the use of their copyrighted computer programs to an end user. The terms of the license will vary substantially based upon the context in which the software is to be used (for example, home, academic, or enterprise), the number of licenses being purchased, the geographic location of the purchaser, the number of activations allowed under the license, as well as other factors, and the associated price of the license may vary substantially based on these factors. Software licenses may also be issued in volume to manufacturers of computers and related computer hardware which allows those manufacturers to include the software with the computer or computer hardware at the time of purchase. When preinstalled on or included with a prebuilt computer or with computer hardware, these software licenses are called original equipment manufacturer (“OEM”) licenses.

46. Your Affiant is further aware that, in order to ensure that a copy of a computer program may be appropriately installed and used in accordance with its license terms, software companies such as Microsoft and Adobe have employed the use of a product key code (Microsoft) or serial number (Adobe) to register and authenticate a software product upon installation. This product key code or serial number is a unique alphanumeric code that corresponds with a specific license and the distinctive associated terms and limitations of that license, such as the type of software program it was intended to be used with, nature of the license, and number of activations, among many other characteristics.

47. Your Affiant is further aware that, during the installation and activation process, the intended user's computer accesses Microsoft and Adobe servers to register this software program and check the product key code or serial number relative to the distinctive characteristics associated with its specific license. Assuming it then passes this verification process, this product key code or serial number unlocks the functionality of the software associated with the license that the licensee has acquired. Depending upon the terms of the associated license, a specific product key code or serial number may allow a limited number of computers on which the licensee may unlock the software, or the use of this software may be otherwise temporally limited based on the nature of this license (if it is a trial license or subscription license). Microsoft or Adobe may block the product key code or serial number if it has been used to activate too many copies of the software, or has been identified as stolen. If the product key code or serial number is rejected by the company servers, the software program will not operate.

#### **LIU AND HIG'S USE OF COMPUTERS**

48. Based on your Affiant's knowledge, training and experience, your Affiant has learned that companies who traffic in illicit and/or counterfeit labels maintain books, records, receipts, notes, ledgers, or electronic data relating to the production, transportation, selling, purchase and distribution of illicit and/or counterfeit labels both in written form, on computers and computer media. In addition, companies who deal in illicit and/or counterfeit labels often maintain address and/or telephone books, rolodex indicia, electronic organizers, telephone paging devices (and the memory thereof), papers, records or electronic data to store the names, addresses, telephone numbers, and pager numbers of co-conspirators, sources of illicit and/or counterfeit labels and customers in written form, on computers and computer media.

49. Based on your Affiant's knowledge, training and experience, your Affiant is aware that vendors of illicit and/or counterfeit labels, obtained on the black market conduct sales, receive payments and make shipping arrangements electronically, using computers and the Internet to conduct these transactions.

50. Based upon your Affiant's knowledge, training and experience, your Affiant believes that LIU and other principals of HIG used a computer to conduct business and arrange for shipments of the illicit and/or counterfeit labels for computer software. Your Affiant believes that LIU and other principals of HIG maintain records on computers and other electronic storage media to generate, store, print and transmit information relating to the production, transportation, selling, purchase and distribution of illicit and/or counterfeit labels.

**METHOD OF SEARCHING AND EXAMINING COMPUTERS AND DIGITAL EVIDENCE**

51. The TARGET ITEMS are currently in the lawful possession of the Department of Homeland Security. It came into the Department of Homeland Security's possession after they were seized from LIU's possession upon his arrest as he traveled into the United States. Therefore, while the Department of Homeland Security might already have all necessary authority to examine the TARGET ITEMS, your Affiant seeks this additional warrant out of an abundance of caution to be certain that an examination of the TARGET ITEMS will comply with the Fourth Amendment and other applicable laws.

52. The TARGET ITEMS are currently in storage at Department of Homeland Security, 4100 N. Mulberry Drive, Suite 225, Kansas City, Missouri. In my training and experience, your Affiant knows that the TARGET ITEMS have been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they

were when the TARGET ITEMS first came into the possession of the Department of Homeland Security.

53. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. *Wireless telephone*: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.
- b. *IP Address*: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static-that is, long-term-IP addresses, while other computers have dynamic-that is, frequently changed-IP addresses.
- c. *Internet*: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

54. Based on my training, experience, and research, your Affiant knows that the TARGET ITEMS (specifically, the Apple MacBook Air and Huawei cellular telephone) have capabilities that allow it to serve as a device to facilitate communications via the Internet, and also retain records of invoices, files containing contraband, and other related documents and

communications. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

55. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

56. There is probable cause to believe that things that were once stored on the TARGET ITEMS may still be stored there, for at least the following reasons:

57. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

58. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space-that is, in space on the storage medium that is not currently being used by an active file-for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a “swap” or “recovery” file.

59. Wholly apart from user-generated files, computer storage media-in particular, computers’ internal hard drives-contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence

can take the form of operating system configurations, artifacts from operating system or application operations, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

60. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

61. *Forensic evidence.* As further described in the respective Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the TARGET ITEMS were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the TARGET ITEMS because:

62. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

63. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

64. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

65. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

66. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

67. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

68. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve




the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the court to authorize execution of the warrant at any time in the day or night.

**CONCLUSION**

69. Your Affiant respectfully requests that a search warrant be issued authorizing Special Agents of Homeland Security Investigations, and other as designated, to search for and to seize items found within the TARGET ITEMS, which is property that constitutes evidence of a criminal offense in violation of 18 USC § 1343, 2318, 1029, 545 and 371, and also contraband, the fruits of a crime, or things otherwise criminally possessed.

FURTHER AFFIANT SAYETH NOT.

  
\_\_\_\_\_  
Carlos Suarez  
Special Agent  
Homeland Security Investigations

Sworn to and subscribed before me this 6th day of <sup>July</sup>~~June~~, 2016 in Kansas City, Missouri.